IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend, LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, MARK HEIL, ALLISON THURMAN, and SHERIE HARRIS, individually and on behalf of all others similarly situated,	)	Case No. 1:21-cv-04976
Plaintiffs,	)	Hon. Nancy L. Maldonado. Presiding Judge
v.	)	
SAMSUNG ELECTRONICS AMERICA, INC., and SAMSUNG ELECTRONICS CO., LTD.	)	
Defendants.	)	

RESPONSE IN OPPOSITION TO
DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

Defendants' (collectively, "Samsung") motion to dismiss misstates what is required to plead violations of Illinois Biometric Information Privacy Act ("BIPA") Sections 15(a) and (b), ignores most of Plaintiffs' factual allegations, and relies on a self-serving declaration that is irrelevant at this stage because Plaintiffs are only required to plead a claim that is plausible on its face to give Samsung "fair notice of what the . . . claim is and the grounds upon which it rests." *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Plaintiffs' complaint easily meets this standard by plausibly alleging that Samsung obtains biometric data through facial recognition software that it embeds in Samsung devices, and Samsung controls ***every*** aspect of that biometric data, from its surreptitious extraction from peoples' photos to Samsung's use of it to create Face Templates that Samsung stores and uses every time a new photo is added to the device. Plaintiffs and the other class members had no ability to control the biometric data Samsung obtained and possessed—indeed, they had no idea it was ever taken from them or where Samsung hid it. Nothing more is required to state a plausible claim under Rule 8. *See id.*

The fact that Samsung carries out its biometric harvesting through its automated software does not change the analysis. If an entity cannot avoid liability under Section 15(b) by hiring an agent to perform the collection, *Rogers v. BNSF Ry. Co.*, 2022 U.S. Dist. LEXIS 45578, at *19 (N.D. Ill. Mar. 15, 2022), Samsung certainly cannot do so through software it developed and preinstalled on every Samsung device, and *still owns* while it is running on the device.

FACTUAL BACKGROUND

A. The Biometric Information Privacy Act.

Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *Consol. Am. Compl.* ¶ 44,

ECF No. 50 (hereinafter, "*Compl.*"). The Legislature sought to protect Illinois residents from the unique threat posed by the unregulated collection and use of biometrics. 740 ILCS 14/5(c).

Under BIPA, private entities are prohibited from capturing, collecting, or otherwise obtaining an individual's biometric data[1] without first complying with specific, easy-to-follow requirements: (1) informing the individual, in writing, that their biometric data is being collected or stored; (2) telling the person why the biometrics are being collected and how long they will be stored; and (3) obtaining a written release for the collection. 740 ILCS 14/15(b). Any private entity that possesses biometric data must also have a publicly available retention policy and must destroy biometric data when it no longer needs it. 740 ILCS 14/15(a).

Like all of BIPA, Sections 15(a)-(b) were designed to protect Illinoisan's rights to control their biometric data. *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019).

B. Samsung's Control and Ownership of Its Proprietary Gallery App.

Samsung is the designer, manufacturer, and vendor of Samsung smartphones and tablets ("Devices"), the most popular of which include its Galaxy line of smartphones and tablets. *See Compl.* ¶ 2. Whenever one purchases a Samsung Device, Samsung retains sole ownership of its preinstalled proprietary software, which cannot be altered or removed by the consumer. *See* ECF No. 17-6 at 4 (¶ 3) (End User Licensing Agreement).[2] All Samsung Devices are manufactured and sold with the Samsung Gallery Application ("Gallery App") pre-installed as the default photo and

[1] BIPA protects two types of data: "biometric identifiers," which include scans of face geometry, and "biometric information," which is any information based on an identifier—no matter how it is created or stored—used to identify a person. 740 ILCS 14/10. Because they are subject to the same requirements, they are collectively referred to herein as "biometric data."

[2] While Samsung's ownership of its software is not alleged in the Complaint, the Seventh Circuit has held "[a] plaintiff need not put all of the essential facts in the complaint; he may add them by … brief in order to defeat a motion to dismiss if the facts are consistent with the allegations of the complaint." *Help at Home, Inc. v. Med. Capital, L.L.C.*, 260 F.3d 748, 752-53 (7th Cir. 2001) (citations and quotations omitted)

video application. *Compl.* ¶ 3. Every photo the user takes or receives is automatically saved to the Gallery App, regardless of whether the user ever opens the Gallery App. *Id.* ¶¶ 51, 52, 58. As described below, Samsung embedded facial recognition software into the Gallery App and uses that software to collect, access, and use biometric data without the user's knowledge.

C. Samsung's Surreptitious Collection of Biometric Data.

Samsung embedded its proprietary facial recognition software into the Gallery App that is preinstalled on Samsung Devices. *Compl.* ¶¶ 4, 6, 50-52. Every time a user takes or receives a photo, Samsung deploys its facial recognition software in order to:

- Scan the photo to determine whether a face is present, and if so, capture the subject's facial geometry by measuring her biometric "facial landmarks"—*i.e.* the distance between, and length, width, and depth of features such as the ears, eyes, nose, mouth, and so forth. *Id.* ¶¶ 4, 52-55.

- Convert those measurements into a unique mathematical representation of the subject's face (*i.e.* a "Face Template") and store the Face Template in a facial database that is maintained at least on the solid state memory of the Samsung Device. *Id.* ¶¶ 4, 53, 55.

- Access and use the Face Templates to identify and group photos of the same individuals by comparing newly-created Face Templates to those stored in the database to determine a match. *Id.* ¶¶ 5, 55, 55 n.14.

- "Tag" the image whenever a match is found and group it with stored images of the identified individual. *Id.* ¶¶ 52, 56.

The process is entirely automated and runs without the user's knowledge or consent each time a new photo arrives on the Samsung Device, *id.* ¶¶ 6, 58, and Samsung Devices cannot be used without automatically collecting biometric data from every stored photo. *See id.* ¶¶ 58-59. Thus, Samsung exercises complete control over whether biometric data is collected, what biometric data is collected, where and how biometric data is stored, how biometric data is stored, how long biometric data is stored, and whether it is encrypted. *Id.* ¶ 60. Samsung then accesses and uses that biometric data in order to recognize, tag, and group images of individuals appearing

in the user's photos. *Id.* ¶¶ 52-56.

Samsung does not disclose or provide notice to users that its facial recognition software automatically harvests their biometric data. *Id.* ¶¶ 6-10, 69-70. Nor does Samsung obtain consent from users before creating, collecting, and controlling their biometric data. *Id.* ¶¶ 6-10, 70, 240-41. Samsung also fails to disclose to nonusers appearing in photographs that it is collecting and controlling their biometric data or obtain their consent to do so. *Id.* ¶ 71. Instead, Samsung misleads users and non-users alike by characterizing its software as mere "image analysis." *Id.* ¶ 7.

Thus, users such as Plaintiffs are unaware of Samsung's biometric harvesting. *Id.* ¶¶ 7, 10, 69-70, 87, 101, 116, 131, 146, 161, 176, 191, 206. They cannot opt out of, disable, modify, or limit the biometric data Samsung creates, collects, and controls. *Id.* ¶¶ 6, 59, 61-63. Nor can they access or delete biometric data from the facial recognition database Samsung also controls. *Id.* ¶ 64.

Samsung previously hosted the "Samsung Cloud," a cloud-storage service that allowed users to automatically back up their entire photo library. *Id.* ¶ 66. In September 2021—shortly after Plaintiff G.T. commenced this action—Samsung disabled the Samsung Cloud. *Id.* ¶¶ 51, 66.

LEGAL STANDARD

A motion to dismiss tests the sufficiency of a complaint rather than its merits. *Gleason v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). In evaluating the sufficiency of a complaint, the Court must view the complaint "in the light most favorable to the plaintiff, taking as true all well-pleaded factual allegations and making all possible inferences from the allegations in the plaintiff's favor." *AnchorBank, FSB v. Hofer*, 649 F. 3d 610, 614 (7th Cir. 2011). "[The Court's] task in reviewing the sufficiency of a complaint is 'necessarily a limited one.

Thus, Samsung's assertions relating to a single self-serving affidavit must be disregarded as they raise factual issues outside the allegations of the Complaint.

Further, "Rule 8 'does not demand that a plaintiff prove [her] case at the outset of the litigation,' nor does it demand that a plaintiff plead facts that she has no way of knowing prior to discovery." *Neals v. Par Tech. Corp.*, 419 F. Supp. 3d 1088, 1092-93 (N.D. Ill. 2019). Instead, the Supreme Court has "reiterated that '[s]pecific facts are not necessary; the statement need only give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.'" *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009) (quoting *Erickson v. Pardus*, 551 U.S. 89, 93 (2007)).

ARGUMENT

I. Plaintiffs Allege Samsung Possessed Their Unique Biometric Data.

Section 15(a) of BIPA requires entities "in possession of [biometric data] to develop" a written, publicly-available policy setting forth retention schedules and guidelines for permanently destroying biometric data "when the initial purpose for collecting or obtaining" that data "has been satisfied, or within 3 years" of the last interaction with the subject, "whichever occurs first," and permanently destroy the data within those timeframes. *See* 740 ILCS 14/15(a). Because there is no dispute Samsung did not develop such a policy or permanently destroy the Class's biometric data within the statutory timeframe, the only issue is whether Plaintiffs allege Samsung "possessed" their data in the first place. *See* ECF No. 55 at 6-7 (hereinafter, "*Mot.*"); *Compl.* ¶ 68. Here, Plaintiffs plead possession under Section 15(a) by alleging Samsung controlled, accessed, received, and exercised dominion over the biometric data. Nothing more is required.

A. Plaintiffs' Allegations Plausibly Suggest That Samsung Stored the Data in Its Samsung Cloud.

Samsung's argument that it does not possess the biometric data because it is stored only on Plaintiffs' Devices contradicts the Complaint. The Complaint alleges the biometric data including Face Templates are "at least" stored locally in centralized databases because Samsung has, during the class period, stored users' photos on the Samsung Cloud, a cloud-based storage system hosted

on Samsung's servers. *Compl.* ¶¶ 51, 66. But the Gallery App connects to the Samsung Cloud to transmit this data to Samsung, and the Gallery App is not only how Samsung captures, obtains, and collects the biometric data, but it is also where Samsung uses the data and stores the photos it "groups" by each subject's unique facial geometry. *Id.* ¶¶ 52-57, 66. Considering those allegations while "making all possible inferences from the allegations in the plaintiff's favor," as required at this stage, Plaintiffs plausibly allege that Samsung possessed the biometric data at issue in this case because the data was transferred to the Samsung Cloud. *See Hofer*, 649 F. 3d at 614; *Neals*, 419 F. Supp. 3d at 1092-93 ("Rule 8 'does not demand . . . that a plaintiff plead facts that she has no way of knowing prior to discovery."). That is further supported by the fact that Samsung discontinued its cloud service in September 2021, shortly after Plaintiff G.T. originally filed suit. *See* ECF No. 2-1 at 1 (state court complaint filed August 11, 2021).[3]

Because Plaintiffs' allegations are sufficient to create a plausible inference that their biometric data was transferred to Samsung's servers, they adequately plead that Samsung possessed the data under Section 15(a).

B. Plaintiffs Allege Samsung Accessed, Used, and Controlled the Data Stored on Samsung Devices.

Even ignoring that the Gallery App is backed up daily to Samsung's databases in the Cloud, Plaintiffs still adequately allege Samsung was in "possession" of the data under BIPA. "The Illinois Supreme Court has held that 'possession, as ordinarily understood, occurs when a person has or takes control of the subject property or holds the property at his or her disposal.'" *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643, 653 (S.D. Ill. 2021) ("*Hazlitt II*") (quoting *People v. Ward*, 830

[3] Samsung's reference to an affidavit showing otherwise is irrelevant. *Mot.* at 2. Plaintiffs have had no opportunity to test this self-serving affidavit through discovery, and the specifics of how Samsung's biometric technology functioned before this case was filed are factual issues that cannot be resolved on a motion to dismiss.

N.E.2d 556, 560 (Ill. 2005)).[4]

Hazlitt II is instructive. That case involved an identical Section 15(a) claim arising from the facial recognition software which, like Samsung's, came "pre-install[ed]" on all Apple phones. 543 F. Supp. 3d at 646. Like Samsung, Apple insisted it could not "possess" biometric data that "remains in the solid-state memory on the [] device, which is owned and controlled by the user." *Id.* at 652. The court rejected that argument, first holding that "possession" as used in Section 15(a) does not even require exclusive control because "[t]he ordinary definition of possession does not require exclusive control, 'and nothing in BIPA indicates that the ordinary definition of possession does not apply.'" *Id.* at 653; *accord Ward*, 830 N.E.2d at 561 (applying "ordinary and popular meaning of 'possession'" because statute contained "no indication . . . legislature intended to depart from" that meaning; thus refusing to apply legal definition requiring exclusive control).

Applying the ordinary definition of possession, the court had no difficulty holding the plaintiffs plausibly alleged Apple "possessed" the biometric data stored locally on their devices:

> Plaintiffs allege Apple "possesses" their biometric data because it has complete and exclusive control over the data on Apple Devices, including what biometric identifiers are collected, what biometric data is saved, whether biometric identifiers are used to identify users (creating biometric information), and how long biometric data is stored. Plaintiffs also claim Apple uses its software to create, gather, and harvest faceprints, which Apple stores in facial recognition databases that Apple provided users no knowledge of or control over, and that Apple alone could access the biometric data or disable its collection. Users also cannot disable the collection of biometric data, cannot limit what information is collected or from whom information is collected, cannot remove the People folder, and cannot delete the database of facial recognition information that Apple creates or any information in that database. Finally, Apple only allows users to use Apple Devices on the condition that it collects biometric data.

[4] "Because the question . . . involves the interpretation of an Illinois statute, [the Court must] apply Illinois's rules of statutory construction." *Zahn v. N. Am. Power & Gas, LLC*, 815 F.3d 1082, 1089 (7th Cir. 2016). Under Illinois' rules of construction, an undefined statutory term such as "possession" must be given "its popularly understood meaning." *Rosenbach*, 129 N.E.3d at 1205 (construing BIPA); *McDonald v. Symphony Bronzeville Park, LLC*, 193 N.E.3d 1253, 1261 (Ill. 2022) ("When construing statutory language, we view [a] statute in its entirety, construing words and phrases in light of other relevant statutory provisions and not in isolation.").

Id. at 653 (internal citations omitted).

As such, Plaintiffs need only allege the defendant "in any way controlled, accessed, received, or extended dominion" over the biometric data. *Mayhall v. Amazon Web Services*, 2022 U.S. Dist. LEXIS 126094, at *19-20 (W.D. Wash. May 24, 2022); *accord Jacobs v. Hanwha Techwin America, Inc.*, 2021 U.S. Dist. LEXIS 139668, at *9 (N.D. Ill. July 27, 2021) (possession occurs when someone "exercise[s] any form of control over the data"); *Smith v. Signature Systems*, 2022 U.S. Dist. LEXIS 34383, at *8-9 (N.D. Ill. Feb. 28, 2022) (possession only requires "some dominion or control" over biometric data).

Here, Plaintiffs' allegations are virtually identical to *Hazlitt II* and therefore meet this requirement. As alleged in the Complaint, Samsung has complete and total control over the biometric data surreptitiously captured using proprietary software that Samsung owned and alone controlled, preventing users from turning it off or disabling it. *Compl.* ¶¶ 52, 58-63. Samsung used its software to harvest biometric data, which data Samsung then used to create and gather face templates that Samsung stored in a database that Plaintiffs had no knowledge of or ability to destroy, access, or control. *Id.* ¶¶ 7-8, 52-54, 64. Samsung further accessed and used that biometric data to tag and group images of individuals appearing in its users' photos. *Id.* ¶¶ 52, 55-56.

Even more specifically, Samsung dictates: (1) whether and when any biometric data is collected; (2) what type of biometric data is collected; (3) whether biometric data is used to identify the subject; (4) whether biometric data is encrypted or protected through some other means; (5) how and where the biometric data is stored; and (6) how long biometric data is stored. *Id.* ¶ 60. The users, by contrast, have no ability to control the data and cannot disable Samsung's pre-installed facial recognition software, limit the type of biometric data collected, or even access (much less delete) the biometric data stored on their Devices. *Id.* ¶¶ 6, 58-59, 61-64. Indeed,

because users lack any modicum of control over the process, their use of Samsung Devices is conditioned on the collection of biometric data. *Id.* ¶ 59. Such secret harvesting of biometric data by large corporations where consumers have no knowledge of or control over their biometric data being taken and used is *exactly* what BIPA was designed to prevent. *See Rosenbach*, 129 N.E.3d at 1206.

Samsung's contention that it did not access the data does nothing more than contradict Plaintiffs' allegations and create a dispute of fact. Plaintiffs allege that Samsung, acting through facial recognition software[5] that it surreptitiously embedded into Samsung Devices, accesses the biometric data stored in the database and uses it to perform a facial recognition analysis each and every time a new photo arrives in the Gallery App on the Device, and then recognize and tag images of individuals in those photos. *Compl.* ¶¶ 4-5, 52, 55-56. This would not be possible if Samsung were incapable of accessing the database in the first place. *See Access Definition*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/access ("access" means "to be able to use, enter, or get near something"); *Vance v. Amazon.com, Inc.*, 525 F. Supp. 3d 1301, 1313 (W.D. Wash. 2021) (denying motion to dismiss Section 15(b) claim based on reasonable inference from allegation biometric data was used in particular way, reasoning that, in order "to have . . . used the data, the defendant necessarily first had to 'obtain' the data" and "Amazon does not explain how it could have . . . used Plaintiffs' facial scans without having first obtained it"); *Vance v. Microsoft Corp.*, 525 F. Supp. 3d 1287, 1297 (W.D. Wash. 2021) (same). Hence, Samsung cannot overcome the fact it controls—and thus possesses—the Class's biometric data.

Nevertheless, Samsung argues that the First District's opinion in *Barnett v. Apple, Inc.*,

[5] Once again, Samsung is responsible for the software it developed, preinstalled on every Samsung Device, can routinely update, and still owns. *Rogers*, 2022 U.S. Dist. LEXIS 45578 at *19 (Defendant is liable under BIPA when it calls the shots regardless if it never possessed or collected the biometric data).

2022 IL App (1st) 220187 compels a different outcome because the *Barnett* court distinguished *Hazlitt II* by noting the biometric data in *Hazlitt II* was stored "in Apple's databases." *Mot.* at 9 (quoting *Barnett*, 2022 IL App (1st) 220187 at ¶ 45). However, the database in *Hazlitt II* was stored in the same location as the one in *Barnett*—"on each Apple device locally." *Hazlitt II*, 543 F. Supp. 3d at 647. The *Barnett* court viewed the database in *Hazlitt II* as "Apple's" database not because of *where* it was physically located, but because unlike the facts in *Barnett*, the database and the data in it were completely controlled by Apple. *See* 2022 IL App (1st) 220187 at ¶ 45. This is illustrated by the omitted part of the sentence Samsung quotes reasoning that in *Hazlitt II* "users had no power to delete the collected information or disable the feature on their devices." *Id.*

Importantly, *Barnett* recognized *Hazlitt II* was sound and did not criticize or disagree with its holding. Instead, *Barnett* focused on the "completely optional" biometric identification feature that provided users with the ability to unlock their iPhones via their fingerprints or facial geometry, and "the user is the sole entity deciding whether or not to use these features." 2022 IL App (1st) 220187 at ¶ 2. The users were also able to stop the collection of biometric data any time they wanted. *Id*. In other words, the court held the plaintiffs possessed their own biometric data because this optional feature provided them with complete control over their data:

> Based on the facts alleged by plaintiffs***, it seems as though Apple designed these features almost with the express purpose of handing control to the user.*** **The features are completely elective.** In fact, the user must undertake a series of steps in order to use them. As plaintiffs' complaint demonstrates with step-by-step photos, the user utilizes her own device in order to capture her own fingerprint or facial image.… **At any time, if she decides that she no longer wants to use these features, she may delete them. There is no allegation that** Apple stores this information on a separate server or that **Apple has ever once prevented a user from deleting her own information**.

Id. ¶ 44 (emphasis added). As such, *Barnett* did not take issue with *Hazlitt's* conclusion that Apple possessed biometric data stored locally where Apple via its software dictates and controls the data,

but instead took issue with the fact that the Apple software at issue in *Barnett* was completely voluntary and controlled by the consumer who could opt in or out and delete the data at any time.

In this case, there is nothing voluntary or optional about Samsung's facial recognition software, and users such as Plaintiffs have no ability to control or even locate (much less delete) the biometric data Samsung stores on their Devices. In short, the technology in *Barnett* provided users with precisely what Plaintiffs here lost—control over their biometric data.

Moreover, the *Barnett* court analyzed the allegations in that case under the fact-pleading standard applicable in Illinois state court, not the notice-pleading standard that applies under Rule 8. *See* 2022 IL App (1st) 220187 at ¶ 30 ("As a result of this difference, we find less persuasive some of the federal cases[.]"); *see also id.* ¶ 53. The Court should reject Samsung's attempt to apply the fact-pleading standard from *Barnett* to Plaintiffs' Complaint in this case.

Samsung's reliance on *Jacobs v. Hanwha* and *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960 (N.D. Ill. 2020) is misplaced as both cases involved attenuated claims against the third-party manufacturers who furnished technology to entities who actually collected the biometric data. *See Heard*, 440 F. Supp. 3d at 963; *Jacobs*, 2021 U.S. Dist. LEXIS 139668 at *2. Indeed, those courts dismissed the Section 15(a) claims precisely because the plaintiffs alleged nothing to show the manufacturer "exercised any form of control over the data or held the data at its disposal." *Heard*, 440 F. Supp. 3d at 968; *Jacobs*, 2021 U.S. Dist. LEXIS 139668 at *9 (same). Neither case held that the plaintiffs possessed their own biometric data. Both cases are inapposite.

Perhaps recognizing this, Samsung contends finding it possessed Plaintiffs' data would be inconsistent with BIPA's Destruction Duty because Samsung would need to devise some method of monitoring users' Devices to ensure the biometric data it systematically harvests is destroyed within the requisite time frame. *Mot.* at 10. But Samsung cannot use BIPA's requirements as both

a sword and a shield, intentionally designing software that secretly collects biometric data on the one hand, while arguing on the other hand that it should be exempt from liability for that violation because compliance would be too difficult. This argument is also factually implausible because Samsung, as the author of the Gallery App, has complete control over when the biometric data is destroyed, and can simply set the App to destroy the data after a specific period of time.[6] *See Compl.* ¶ 60 (Samsung "[c]ontrols how long Biometrics are stored").

Samsung's argument is also legally wrong and no court has accepted it. *See, e.g.*, *Johnson v. NCR Corp*., 2023 U.S. Dist. LEXIS 19327, at *6 (N.D. Ill. Feb. 6, 2023) (rejecting argument vendor could not be liable under Section 15(b) because it lacked direct relationship with plaintiffs and means for determining when "initial purpose" for collecting data was satisfied, reasoning "BIPA's text does not suggest a carveout for third-party vendors"). As the Illinois Supreme Court put the point, "compliance [with BIPA] should not be difficult. Whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded." *Rosenbach*, 129 N.E.3d at 1207.

In any event, Samsung's purported concerns are misdirection because *Barnett* provides a simple solution—cede control to the user. All Samsung needs to do is disclose the facial recognition software to users, allow them to choose whether to enable the software, and permit them to destroy their biometric data if they choose. Here, Samsung did the opposite.

Because Plaintiffs allege more than enough facts to show Samsung exerted "some" control or dominion over their biometric data at this stage of the litigation, they have adequately pled "possession" under Section 15(a) and Samsung's motion should be denied.

[6] Of course, the fact that Samsung routinely changes software illustrates it has the control needed to copy and move Plaintiffs' biometric information anytime and any way it wants via an update.

II. Plaintiffs Adequately Allege a Section 15(b) Claim.

Section 15(b) provides a private entity cannot "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" without the person's prior informed written consent. 740 ILCS 14/15(b).

As set forth in detail above, the Complaint details precisely how Samsung's facial recognition software captures, collects, and obtains the Class's biometric data without their knowledge or consent. *Compl.* ¶¶ 4-10, 52-59, 69-70. Because nothing more is required to trigger liability under Section 15(b), *see* 740 ILCS 14/15(b), it makes no difference whether Samsung stored this highly-sensitive data on its servers or in a facial recognition database it controls on each user's individual Device. Indeed, as the Illinois Supreme Court recently held in *Cothron v. White Castle*, 2023 IL 128004, a private entity can capture or collect biometric data without storing the data at all.

Cothron involved a biometric identification system that required employees to provide an initial fingerprint scan, which a third-party vendor stored in an offsite database. *Id.* ¶ 23. The system did not store the employee's subsequent fingerprint scans; instead, those "authentication" scans were just compared against the stored copy to verify the employee's identity. *See id.*

The Illinois Supreme Court first held the term "collect," as used in Section 15(b), means "to receive, gather, or extract from a number of persons or sources" whereas "'[c]apture' means 'to take, seize, or catch.'" *Id.* ¶ 23. From there, the Court rejected White Castle's attempt to equate those terms with "storage," explaining Section 15(b)(2) "distinguishes collection from storage." *Id.* The court held White Castle captured or collected the plaintiff's fingerprints every time she scanned her fingerprints that were not stored—not just when White Castle obtained the copy that its vendor stored in a database. *See id.* ¶ 24 ("This is true the first time an entity scans a fingerprint

. . . , but it is no less true with each subsequent scan[.]"); *see also id.* ¶ 45 (holding a separate Section 15(b) "claim accrues under the Act with *every scan* . . . of biometric identifiers or biometric information without prior informed consent") (emphasis added). *Cothron* held that it's a violation for the subsequent scans that were not stored because they were still collected or captured. Thus, storage cannot be a requirement for a Section 15(b) claim. Indeed, storage is regulated by an entirely separate provision—Section 15(e). *See* 740 ILCS 14/15(e).

Instead, Plaintiffs need only allege Samsung captured, collected or otherwise obtained their biometric data. *See* 740 ILCS 14/15(b). Plaintiffs have clearly done so here, as the Complaint extensively details how Samsung collected the biometric data by extracting scans of facial geometry from myriad people and sources—*i.e.* every individual appearing in any photo on the user's Samsung Device. *Compl.* ¶¶ 4, 52-57, 71. Because none of this is voluntary, Samsung "captured" the biometric data by seizing it from those photos without the user's knowledge or consent (written or otherwise). *Id.* ¶¶ 4, 6-10, 9, 58-59, 62-63.

In addition, Samsung "obtains" the biometric data within the meaning of Section 15(b) because "[t]he active verbs used in section 15(b)—collect, capture, purchase, receive, and obtain—all mean to gain control." *Cothron*, 2023 IL 128004 at ¶ 16. Samsung controlled every aspect of the biometric data, from its surreptitious extraction from users' and non-users' photos to its use of that data to create the Face Templates, and Samsung owns the software. *See supra* § I; *Control Definition*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/control ("control" means "to exercise restraining or directing influence over" or "to have power over.").

Otherwise, Samsung could not have created the Face Templates in the first place. *See, e.g.*, *Amazon.com*, 525 F. Supp. 3d at 1313 (denying motion to dismiss Section 15(b) claim, explaining that, in order "to have . . . used the data, the defendant necessarily first had to 'obtain' the data");

Microsoft, 525 F. Supp. 3d at 1297 (same).

To the extent Samsung suggests "obtaining" biometric data requires an "active step," it took such as step. Plaintiffs allege Samsung secretly accessed and used the biometric data to recognize, tag, and group images of individuals who appear in the user's photographs. *Compl.* ¶¶ 55-57. Samsung's actions even satisfy its own authorities. *See, e.g.*, *Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021) (amended complaint alleged active step by describing how biometric medication dispenser leased by plaintiff's employer captured her fingerprints and transferred them to servers). Here, Plaintiffs allege Samsung embeds into all Samsung Devices facial recognition software that automatically harvests biometric data from every photo stored on the Device and not only conceals this from users, but prevents them from disabling the process or destroying that information. *Compl.* ¶¶ 7, 58-59, 63-64. If that's not an "active step," then nothing is. In short, Plaintiffs' allegations are more than sufficient to state a Section 15(b) claim.

Lest there be any doubt, other courts considering identical claims have reached the same conclusion. In *Hazlitt I*, for instance, the court roundly rejected Apple's attempt to evade liability under Section 15(b) simply because the biometric data captured through its facial recognition software was "stored locally" on the user's device. *Hazlitt v. Apple Inc.*, 500 F. Supp. 3d 738, 750 (S.D. Ill. 2020) ("*Hazlitt I*"). The court held the defendant "collected, possessed, and exercised exclusive control over the biometric data extracted from Plaintiffs' photos within the Photos app," *id.* at 751, and refused to dismiss the Section 15(b) claim, reasoning:

> Plaintiffs allege that Apple both "collected" and "possessed" their biometric data using proprietary software that Apple owned, exclusively controlled, and barred individual users from accessing, removing, or disabling. More specifically, Plaintiffs allege that Apple used its software to create, gather, and harvest faceprints, which Apple stored in facial recognition databases that Apple provided users no knowledge of, or control over, and Apple alone could access the biometric

> data or disable its collection. Plaintiffs assert that Apple is subject to BIPA liability from its collection and possession of Plaintiffs' biometric data based on common law agency principles. In furtherance of this theory, Plaintiffs allege that Apple's software cannot be used as intended without biometric data automatically being collected, that device users had no ability to disable the collection (or notice of collection), and Apple prevents users from accessing, disabling, or altering the software.

Id. at 750 (internal citations omitted). As discussed *supra* § I, those facts are materially identical to what Plaintiffs allege here.[7]

The court in *Svoboda, et al. v. Amazon.com, Inc., et al.*, No. 1:21-cv-05336 (N.D. Ill) reached the same result. Despite the defendant's argument that the biometric data obtained through its "virtual try on" software remained solely on the user's device, the court found the plaintiffs adequately pled a Section 15(b) claim and denied the motion to dismiss, holding that "storage is not a necessary component of either the 15(a) or the 15(b) causes of action." *See id.*, Hr'g Tr. at 7:12-16, Apr. 28, 2022, attached as **Exhibit 1**. Similarly, in *Rogers v. BNSF*, the court rejected the defendant's attempt to evade liability on grounds that its vendor was the one who collected and stored the fingerprints. *See* 2022 U.S. Dist. LEXIS 45578 at *19. Instead, the court denied the defendant's motion for summary judgment based on evidence the defendant "ultimately called the shots on whether and how the biometric data was collected." *Id.* (holding "a jury could find [the defendant], and not just [its vendor], violated BIPA, whether by collecting, capturing, receiving through trade, or otherwise obtaining the biometric information at issue"). Hence, for the purpose of the Section 15(b) analysis, the critical issue is not whether the defendant stored the biometric

[7] Samsung's reliance on *Hazlitt III* is misplaced because that opinion was about an amendment to the complaint that occurred **after** the plaintiffs obtained discovery into how Apple's software at issue worked. *Doe v. Apple Inc.*, 2022 U.S. Dist. LEXIS 222988, at *2-3 (S.D. Ill. Aug. 1, 2022) (*Hazlitt III*); *see id.* at *9-10 (treating amended counts for Section 15(a) and 15(b) as new claims because both alleged new facts showing Apple stored biometric data in its servers). As such, *Hazlitt III* has no bearing on *Hazlitt I* or *Hazlitt II* discussed above, both of which were decided based on the claims that were alleged **before** any discovery had occurred, which claims are substantively identical to the claims alleged here. If anything, *Hazlitt III* only underscores that Plaintiffs here should be allowed discovery into how Samsung's system works.

data (on its servers or anywhere else), but whether the defendant is who ultimately controlled the process and data that was obtained through the process. That is exactly what Plaintiffs allege here.

Once again, *Barnett* does not compel a different result for several reasons.

First, Samsung's reliance on *Barnett* is misplaced because *Barnett*'s construction of key terms in Section 15(b) conflicts with the Illinois Supreme Court's holding in *Cothron*. Specifically, *Barnett's* construction of "collect" required the data to be gathered in a single location, 2022 IL App (1st) 220187 at ¶ 49, but *Cothron* held "collect" does not require aggregating the data into a single database and instead simply means "to receive, gather, or extract from a number of persons or other sources." 2023 IL 128004, ¶ 23. Similarly, *Barnett* construed "capture" to require that the data be recorded in a file, 2022 IL App (1st) 220187 at ¶ 48, but *Cothron* held that capture merely "means 'to take, seize, or catch.'" 2023 IL 128004, ¶ 23. *Cothron* controls such that Samsung is wrong when it asserts Plaintiffs cannot allege the data is captured or collected when it is stored locally on numerous Devices. *See Williams, McCarthy, Kinley, Rudy & Picha v. Nw. Nat'l Ins. Grp.*, 750 F.2d 619, 624 (7th Cir. 1984) ("[T]he Illinois Supreme Court is the final authority on the meaning of Illinois statutes"); *Straits Fin. LLC v. Ten Sleep Cattle Co.*, 900 F.3d 359, 369 (7th Cir. 2018) ("We apply the relevant decisions of the Illinois Supreme Court[.]").

Second, to the extent *Barnett* holds a plaintiff cannot demonstrate the defendant captured or collected biometric data that it never possessed, *see Barnett*, 2022 IL App (1st) 220187 at ¶ 55, Plaintiffs have adequately alleged Samsung exclusively controls—and thus possesses—the biometric data systematically harvested through its facial recognition software, *see supra* § I.[8]

Third, *Barnett* is also distinguishable on its facts. While the court noted the biometric data collected via Apple's security feature was stored locally on the user's devices, its ruling on the

[8] Once again, the *Barnett* court was applying Illinois' fact-pleading standard, not Rule 8's notice-pleading standard that applies to the instant case. *See Barnett*, 2022 IL App (1st) 220187 at ¶ 30.

Section 15(b) claim ultimately turned on the same facts that doomed the Section 15(a) claim—the users' complete control over the optional biometric identification system. *Barnett*, 2022 IL App (1st) 220187 at ¶ 52 ("[T]he feature is wholly optional, the information is stored exclusively on plaintiffs' devices, and they may delete the information at will."); *id.* ¶ 2 ("these features are completely optional" and "the user is the sole entity *deciding* whether or not to use *these features*"). Given those facts, the court concluded "[t]he device and the software are the tools, but it is the user herself who utilizes these tools to capture her own biometric information." *Id.* ¶ 44.

Here, however, Plaintiffs had no way of knowing the mere act of taking or receiving a picture would result in the collection of their biometric data because Samsung actively conceals its facial recognition software from users. Plaintiffs did not *decide* to collect their own biometric data (or anyone else's appearing in their photos), they simply decided to save photos to their Samsung Devices. Any biometric harvesting that occurred was completely out of Plaintiffs' control—they did not know it was occurring, nor did they have any means of modifying or disabling Samsung's facial recognition software. *Compl.* ¶¶ 4, 6-7, 61-64. Even the drastic step of destroying their Samsung Devices cannot stop the process because simply posing for a picture taken by another Samsung user will result in Plaintiffs' biometric data being collected on *that* user's Samsung Device or the Samsung cloud. *See id.* ¶ 81 (alleging Plaintiff G.T.'s biometric data was harvested from photos of her stored on relatives' Samsung Devices).

Put simply, a person cannot "exercise directing influence over" or "have power over" something the person does not even know exists and has no ability to disable or access. *See Control Definition*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/control. That is the factual scenario alleged here, in contrast to the facts of *Barnett*, and in contrast to Samsung's Microsoft Word analogy where the person *decided* to use Word for the express purpose of creating

a file (*i.e.* brief) that the person *knows* exists and the person intentionally created, decided to save, decided where to save, and had the power to delete at any time. Samsung's analogy in which one knowingly creates and controls data in every way mirrors the facts of *Barnett*—not the facts here or in *Hazlitt I* and *Hazlitt II*. The bottom line is that Samsung—not the user—is the one capturing and collecting biometric data.

Finally, the fact that Samsung carries out its biometric harvesting through its automated facial recognition software does not change the analysis. If an entity cannot avoid liability under Section 15(b) by hiring an agent to perform the collection, *Rogers*, 2022 U.S. Dist. LEXIS 45578 at *19, Samsung certainly cannot do so through a sophisticated piece of software it developed and preinstalled on every Samsung Device, and *still owns* while it is running on the Device.

The notion that Plaintiffs "used" Samsung's facial recognition software to collect their own biometric data or "decided" to do so is simply not what the Complaint alleges, it ignores the collection of non-users' biometrics and it should be rejected outright, especially when "making all possible inferences from the allegations in the plaintiff's favor" as the Court must do at this stage. *See Hofer*, 649 F. 3d at 614. Accordingly, the Motion should be denied.

III. Plaintiffs Allege Samsung Captures, Collects, and Obtains Two Forms of Data Regulated by BIPA—Scans of Face Geometry and Face Templates.

BIPA protects two distinct types of information: biometric identifiers; and biometric information. *See* 740 ILCS 14/10. BIPA broadly defines "biometric information" as any "information … based on an individual's biometric identifier *used to identify an individual*." *Id.*

On the other hand, "biometric identifier" is expressly defined to include six specific items: (1) fingerprints; (2) voiceprints; (3) retinal scans; (4) iris scans: (5) scans of hand geometry; and (6) scans of facial geometry. *Id.* Nothing in the definition of "biometric identifier" requires any of those items to be used (or be capable of being used) to identify a person. *See id.*

Here, Plaintiffs allege Samsung captures and collects both types of data.

First, Plaintiffs expressly allege Samsung's facial recognition software systematically captures scans of facial geometry, *Compl.* ¶¶ 4, 7, 53, 55, 57, which is one of the six items explicitly listed in BIPA's definition of "biometric identifier." *See* 740 ILCS 14/10; *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) ("Each specific item on the list, not surprisingly, fits within the meaning of the term 'biometric identifier' ….''). Nothing more is required.

To the extent Samsung is suggesting that, in order to allege a "biometric identifier" was involved, Plaintiffs must allege something more, courts have consistently rejected that exact argument. *See, e.g.*, *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 518 n.2 (N.D. Ill. 2022) ("The collection of a voiceprint—which is explicitly included in the definition of 'biometric identifier'—without consent, *even if not collected for the purpose of identifying that person*, is a violation of the statute.") (emphasis added); *accord Goree v. New Albertsons, L.P., d/b/a Jewel Osco*, No. 22-cv-01738 (N.D. Ill.), Hr'g Tr. at 14:20-15:5, 15:11-17:10, Mar. 8, 2023, (denying motion to dismiss), attached as **Exhibit 2**; *Hazlitt I*, 500 F. Supp. 3d at 749 ("Apple reads the word 'identifier' to exclude data that does not identify an actual person. This Court finds that interpretation too narrow.") (internal citation omitted).[9] This Court should do so as well.

***Second*,** the Face Templates Samsung generates from scans of facial geometry constitute "biometric information." *See* 740 ILCS. Plaintiffs allege Samsung creates each Face Template by converting a scan of the subject's facial geometry into a mathematical representation of the subject's face. *Compl.* ¶¶ 4, 53, 55. Samsung does not suggest otherwise, but instead appears to contend the Face Templates are not biometric information because Plaintiffs allege Samsung uses

[9] *Cf. Witbrod v. Blitt & Gaines, P.C.*, 2015 U.S. Dist. LEXIS 56428, at *4 (N.D. Ill. Apr. 29, 2015) (A violation of one of the enumerated acts constitutes a violation of the ICFA without the need to show it meets the elements of an ICFA claim.).

these datasets to "recognize"—rather than "identify"—the subject. *Mot.* at 13. Samsung's argument is misdirection because the two terms are synonymous. *See Identify Definition*, Merriam-Webster.com, https://www.merriam-webster.com/thesaurus/identify.

Moreover, while Samsung denies using the Face Templates to identify any particular person, *Mot.* at 4, that denial contradicts the Complaint. Plaintiffs allege Samsung creates the Face Templates for the sole purpose of identifying the person—that is, Samsung uses the Face Templates to recognize the person among the sea of faces appearing on the hundreds (if not thousands) of photographs stored in the Gallery App, all of which are grouped into a "stack" underneath a circular frame showing the face of the "identified individual." *Compl.* ¶¶ 5, 55-56. In other words, Samsung's software is designed to and does identify people based on certain attributes of their physical appearance, which is no different than when a witness "identifies" a suspect from a police lineup. Nothing more is required to plead "biometric information" as defined by BIPA.

While Samsung argues "biometric information" must be able to identify the subject *by name* without any additional data points, *Mot.* at 13, BIPA's definition of "biometric information" contains no such requirement. 740 ILCS 14/10. Samsung's authorities likewise confirm it makes no difference whether the facial recognition software can link the Face Templates with a specific name absent some additional data provided by the end-user. *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1158 (N.D. Cal. 2016) (software made "suggestions" about the identities of individuals based on "tagging," which "is when a user identifies by name other Facebook users and non-users who appear in the photographs"); *Monroy v. Shutterfly, Inc.*, 2017 U.S. Dist. LEXIS 149604, at *2 (N.D. Ill. Sep. 15, 2017) (denying motion to dismiss BIPA claim where provided users names used to match biometric face templates). That's just how biometric technology works—no system can determine a name based solely on a mathematical

representation of a face. Thus, the fact that the *Rosenbach* plaintiff's mother supplied her son's name on his application for a season pass did not stop the Illinois Supreme Court from holding the digital copy of his thumbprint qualifies as biometric information. *See* 129 N.E.3d at 1200, 1203.

Despite trying to bolster its argument by noting the facial recognition software in *Rivera*, *Facebook*, and *Shutterfly* tied the subject's name to her face template using data stored in those defendants' servers, *Mot.* at 14, Samsung does not—and cannot—explain how the location of the user-generated name information the software uses to perform this function matters under Section 15(a) or (b).

Because the Complaint alleges Samsung captures and collects biometric identifiers *and* biometric information, the Motion to dismiss should be denied.

CONCLUSION

For all of the foregoing reasons, Samsung's motion to dismiss should be denied.

Dated: March 15, 2023

Respectfully submitted,

G.T., BY AND THROUGH NEXT FRIEND LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, MARK HEIL, ALLISON THURMAN, AND SHERIE HARRIS, individually and on behalf of all others similarly situated, Plaintiffs

By: /s/ Gregg M. Barbakoff

Keith J. Keogh
Theodore H. Kuyper
Gregg M. Barbakoff
KEOGH LAW, LTD.
55 W. Monroe Street, Suite 3390
Chicago, Illinois 60603
(312) 726-1092
keith@keoghlaw.com
tkuyper@keoghlaw.com
gbarbakoff@keoghlaw.com

Christian Levis (*pro hac vice forthcoming*)
Amanda Fiorilla (*pro hac vice forthcoming*)
Rachel Kesten (*pro hac vice forthcoming*)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, New York 10601
(914) 997-0500
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that, on **March 15, 2023**, I caused a copy of the foregoing document, along with any attached exhibits, to be served upon all counsel of record via electronic filing using the CM/ECF system.

/s/ Gregg M. Barbakoff